ADVANCES IN MATHEMATICS 19, 1–5 (1976)

Pythagorean Triples, Gaussian Composition, and Spinor Genera

GORDON PALL

Department of Mathematics, Louisiana State University,

Baton Rouge, Louisiana 70803

DEDICATED TO THE MEMORY OF PASQUALE PORCELLI

It has long been known that the integers z, r, s satisfying

$$z^2 = r^2 + s^2, \qquad (r, s) = 1,\ z \text{ positive},\ r \text{ odd, and } s \text{ even}, \tag{1}$$

are expressed by the formulas

$$z = u^2 + v^2, \quad r = u^2 - v^2, \quad s = 2uv, \quad \text{where } u + v \text{ is odd and } (u, v) = 1. \tag{2}$$

Ten papers noting divisibility properties of r, s, or z by 3, 5, 7, or 11 are listed in [1, vol. 1, p. 171]. Such properties can be deduced from (2) by studying possible residues of u^2 and v^2. For example, Lévy showed that 11 divides $5r \pm s$ or $5s \pm r$ if rsz is prime to 11. It seems to have been overlooked that the results differ according as z is a quadratic residue or a quadratic nonresidue modulo p. We will prove the existence of a general result for any odd prime p, the phenomenon being related to properties of spinor genera of binary quadratic forms; and will set up an algorithm for finding, for any given p, the sets of residues modulo p that are possible. Our procedure here illustrates neatly the power of Gaussian composition, which has only recently begun to be properly understood (cf. [4]).

THEOREM 1. *Let p be an odd prime. Denote by S_j ($j = 1$ or -1) the set of possible residues of the pair r, s modulo p when the Legendre symbol $(z : p)$ has the value j. Then, S_1 and S_{-1} are disjoint.*

This is trivial when $p \equiv 1 \pmod 4$. For then, $r^2 + s^2$ is a fourth-power residue of p when $(z : p) = 1$ and is a quadratic, but not a fourth-

power, residue of p when $(z : p) = -1$. But the latter category does not exist when $p \equiv 3 \pmod 4$. We will now prove Theorem 1 for any odd prime p, by a method that will yield an algorithm for finding the residues in each S_j.

It will be useful to rewrite (1) as follows:

$$z^2 = a^2 + 4b^2, \qquad (a, 2b) = 1, \qquad (z, 2p) = 1, \quad z > 0. \tag{3}$$

If p divides b, then z^2 is primitively represented by the principal form $x^2 + 4p^2y^2$ of determinant $4p^2$. For reasons soon to be clear, we will designate this form by f_∞. If p does not divide b, we can choose k so that $kb \equiv a \pmod p$ and have z^2 primitively represented by the form $f_k = (px + ky)^2 + 4y^2$; and we can regard k as merely a residue modulo p. Since $(z, p) = 1$, $1 + (-1 : p)$ residues k are excluded and the f_k are primitive. The number of such forms f_k (counting f_∞) is $p - (-1 : p)$. As it happens, these forms appear in a special case in [2, Section 2], from which it now follows (since $x^2 + 4y^2$ has only the trivial unimodular automorphs I and $-I$) that there are exactly $p - (-1 : p)$ positive-definite primitive classes of determinant $4p^2$, each containing a unique form f_k. The set H of these classes forms an abelian group under composition. They comprise two genera, the first genus (that of f_∞) having the generic character $(f : p)$ equal to 1, the second genus having $(f : p) = -1$. Since f_0 represents 4 and $(4 : p) = 1$, f_0 is in the first genus and consequently, by [3], that genus splits into two spinor genera, the first of which (containing f_∞) comprises the classes that are fourth powers under composition and that can be characterized as representing primitively only squares z^2 $(z > 0)$, such that $(z : p) = 1$; and the second spinor genus consisting of the squares that are not fourth powers represents primitively only squares z^2 $(z > 0)$ such that $(z : p) = -1$. Since each f_k belongs to only one of the two spinor genera, Theorem 1 follows.

Thus, $(z : p) = 1$ if p divides s (the form being f_∞). Comparing the expressions $(px + ky)^2 + 4y^2$ and $r^2 + s^2$, we see that $r \equiv ks/2 \pmod p$ is impossible if $(z : p) = 1$ and f_k is in the second spinor genus, or if $(z : p) = -1$ and f_k belongs to the first spinor genus. Thus, to find the residue sets S_1 and S_{-1}, we need only find to which spinor genus each form f_k belongs. This is made easy by the following result.

THEOREM 2. *The abelian group H constituted by the primitive positive-definite classes of determinant $4p^2$ under composition coincides with the*

group G whose elements are the suffixes k of the forms f_k (including ∞ and excluding $k^2 + 4 \equiv 0 \bmod p$) under the operation $\circ$, defined as follows:

$$h \circ k = \frac{hk - 4}{h + k}, \qquad \text{if} \quad h \neq -k; \; h \circ -h = \infty; \; \infty \circ h = h = h \circ \infty, \quad \infty \circ \infty = \infty. \tag{4}$$

The group G is cyclic.

Proof. By the elements of the theory of composition, f_∞ is the identity and f_h and f_k are inverses if $k \equiv -h \pmod p$. Given h and k such that $k \not\equiv -h \pmod p$, we will determine m so that $f_h \cdot f_k = f_m$ under a Gaussian bilinear substitution. (An account of Gaussian composition will be found in [4].) We need only choose m so that the bilinear expressions for x'' and y'' in terms of x and y, x' and y', obtained by equating real and imaginary parts in

$$px'' + my'' + 2iy'' = (yx + hy + 2iy)(yx' + ky' + 2iy') \qquad (\text{where } i^2 = -1), \tag{5}$$

will have integral coefficients. This gives

$$m \equiv (hk - 4)/(h + k) \pmod p. \tag{6}$$

All of Theorem 2 follows except the property that G is cyclic. Let $h^{(n)}$ denote the nth power of the element h of G. We will prove that for any positive integer n, the number of elements of G *exactly* of order n does not exceed n. From this will follow that G is cyclic, since otherwise, by the fundamental theorem on abelian groups, there would be a q-by-q subgroup, where q is some prime, and hence, at least $q^2 - 1$ elements exactly of order q. To proceed, if $h \neq \infty$,

$$h^{(2)} = (h^2 - 4)/2h,$$

and by an easy induction, if $n > 0$ and h is not of order less than n, then $h^{(n)} = A_n/B_n$, where A_n is a polynomial in h with leading term h^n and B_n is a polynomial in h with leading term nh^{n-1}. Thus, except possibly when $n = p$ and B_p is the zero polynomial, there are at most $n - 1$ elements h exactly of order n. Also, since the group order $p - (-1 : p)$ is not divisible by p, there are no elements exactly of order p. This completes the proof of Theorem 2.

Thus, in order to find the S_j, we need only find a generator of G, or of its subgroup of squares. Doing this for small primes p provides

a good exercise for beginners in group theory. We include the results up to $p = 31$ (see Table I).

From Table I it follows that if $p = 3$ or 5, p divides the even number s if $(z : p) = 1$, the odd number r if $(z : p) = -1$; if $p = 7$, p divides rs if $(z : p) = 1$, $r \pm s$ if $(z : p) = -1$; if $p = 11$, p divides s or $r \pm 2s$ if $(z : p) = 1$, $r \pm hs$ $(h = 0$ or $5)$ if $(z : p) = -1$;...: if $p = 31$, p divides rs or $r \pm hs$ $(h = 1, 9,$ or $7)$ if $(z : p) = 1$, $r \pm hs$ $(h = 15, 2, 3,$

TABLE I

Generators of Small Primes

p	If $(z : p) = 1$, $k =$	If $(z : p) = -1$, $k =$
3 or 5	∞	0
7	∞, 0	± 2
11	∞, ± 4	0, ± 1
13	∞, ± 6	0, ± 5
17	∞, 0, ± 2	± 3, ± 7
19	∞, ± 1, ± 8	0, ± 4, ± 9
23	∞, ± 3, ± 9	± 2, ± 5, ± 10
29	∞, ± 3, ± 4, ± 13	0, ± 1, ± 7, ± 11
31	∞, 0, ± 2, ± 13, ± 14	± 1, ± 4, ± 6, ± 11

or 10 if $(z : p) = -1$. It is easily shown that f_0 is in the first or second spinor genus, according as $(2 : p)$ is 1 or -1; and that if $(2 : p) = 1$, the statement for each S_j is symmetric in r and s; but if $(2 : p) = -1$, the statement for S_{-1} is obtained from that for S_1 by interchanging r and s.

It can be deduced from (2) that $s \equiv 0$ or 4 mod 8 according as $z \equiv 1$ or 5 mod 8. This also is a spinor-generic phenomenon. For, $f = x^2 + 64y^2$ and $g = (2x + y)^2 + 16y^2$ (which arise from $x^2 + 4y^2$ by transformations of determinant 4) are in different spinor genera: if z is odd and positive, z^2 cannot be primitively represented by f unless $z \equiv 1$ mod 8, nor by g unless $z \equiv 5$ mod 8.

References

1. L. E. Dickson, "History of the Theory of Numbers" (reprint), Stechert, New York, 1934.

2. G. PALL, Binary quadratic discriminants differing by square factors, *Amer. J. Math.* **57** (1935), 789–799.
3. D. R. ESTES AND G. PALL, Spinor genera of binary quadratic forms, *J. Number Theory* **5** (1973), 421–432.
4. G. PALL, Aspects of Gaussian composition, *Acta Arith.* **24** (1973), 401–409.